Current Technologies
Computer Learning Centers

CompTIA

6210 Central Ave, Portage, IN. 46368 Phone: 219.764.3800 Fax: 219.764.3805 Web: http://www.ctclc.com

CompTIA Penetration Tester (PenTest+)

This course provides the knowledge needed to plan and perform penetration tests and other security engagements, using a vendor-neutral format. This includes planning engagements, performing reconnaissance to find vulnerabilities in a target organization, exploiting vulnerable targets, and creating follow-up reports.

How you'll benefit

This class will help you:

- Learn general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

Why Attend with Current Technologies CLC

- Our Instructors are in the top 10%
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs Run up to Date Code for all our courses

Objectives

Upon completing this course, the student will be able to meet these objectives:

- Plan and scope penetration tests
- Conduct passive reconnaissance
- Perform non-technical tests to gather information
- Conduct active reconnaissance
- Analyze vulnerabilities
- Penetrate networks
- Exploit host-based vulnerabilities
- Test applications
- Complete post-exploit tasks
- Analyze and report penetration test results

Course Duration

5 day

Course Price

$2,895.00

Methods of Delivery

- Instructor Led
- Virtual ILT
- On-Site

Certification Exam

PT0-001

Who Should Attend

The job roles best suited to the material in this course are:

CompTIA Penetration Tester (PenTest+)

- This course is intended if you plan to become a certified penetration tester, or if you are a security professional who wishes to understand cybersecurity from an offensive perspective.
- Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability

Perquisites

To fully benefit from this course, you should have the following knowledge:

- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.

Outline

Module 0: Introduction

- Course setup

Module 1: Engagement planning

- Assessment types and goals
- The penetration testing process
- Documentation and planning
- Engagement scope
- Scripting

Module 2: Reconnaissance

- Reconnaissance techniques
- OSINT gathering

Module 3: Active Reconnaissance

CompTIA Penetration Tester (PenTest+)

- Network scanning
- Vulnerability scanning
- Application testing

Module 4: Leveraging target information

- Vulnerability analysis
- Exploitation techniques

Module 5: Exploiting organizational vulnerabilities

- Social engineering
- Physical security attacks

Module 6: Exploiting network vulnerabilities

- Network attacks
- Wireless attacks

Module 7: Exploiting applications

- Attacking insecure code
- Attacking web applications

Module 8: Host exploitation

- Finding host vulnerabilities
- Operating system exploits
- Post-exploitation techniques

Module 9: Engagement follow-up

- Report preparation
- Remediation and follow-up